North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions

Published: 2018-09-06 · Archived: 2026-04-06 02:04:09 UTC

A criminal complaint was unsealed today charging Park Jin Hyok (박진혁; a/k/a Jin Hyok Park and Pak Jin Hek), a North Korean citizen, for his involvement in a conspiracy to conduct multiple destructive cyberattacks around the world resulting in damage to massive amounts of computer hardware, and the extensive loss of data, money and other resources (the "Conspiracy").

The complaint alleges that Park was a member of a government-sponsored hacking team known to the private sector as the "Lazarus Group," and worked for a North Korean government front company, Chosun Expo Joint Venture (a/k/a Korea Expo Joint Venture or "KEJV"), to support the DPRK government's malicious cyber actions.

The Conspiracy's malicious activities include the creation of the malware used in the 2017 WannaCry 2.0 global ransomware attack; the 2016 theft of $81 million from Bangladesh Bank; the 2014 attack on Sony Pictures Entertainment (SPE); and numerous other attacks or intrusions on the entertainment, financial services, defense, technology, and virtual currency industries, academia, and electric utilities.

The charges were announced by Attorney General Jeff Sessions, FBI Director Christopher A. Wray, Assistant Attorney General for National Security John C. Demers, First Assistant United States Attorney for the Central District of California Tracy Wilkison and Assistant Director in Charge Paul D. Delacourt of the FBI's Los Angeles Field Office.

In addition to these criminal charges, Treasury Secretary Steven Mnuchin announced today that the Department of the Treasury's Office of Foreign Assets Control (OFAC) designated Park and KEJV under Executive Order 13722 based on the malicious cyber and cyber-enabled activity outlined in the criminal complaint.

"Today's announcement demonstrates the FBI's unceasing commitment to unmasking and stopping the malicious actors and countries behind the world's cyberattacks," said FBI Director Christopher Wray. "We stand with our partners to name the North Korean government as the force behind this destructive global cyber campaign. This group's actions are particularly egregious as they targeted public and private industries worldwide – stealing millions of dollars, threatening to suppress free speech, and crippling hospital systems. We'll continue to identify and illuminate those responsible for malicious cyberattacks and intrusions, no matter who or where they are."

"The scale and scope of the cyber-crimes alleged by the Complaint is staggering and offensive to all who respect the rule of law and the cyber norms accepted by responsible nations," said Assistant Attorney General Demers. "The Complaint alleges that the North Korean government, through a state-sponsored group, robbed a central bank and citizens of other nations, retaliated against free speech in order to chill it half a world away, and created disruptive malware that indiscriminately affected victims in more than 150 other countries, causing hundreds of millions, if not billions, of dollars' worth of damage. The investigation, prosecution, and other disruption of

malicious state-sponsored cyber activity remains among the highest priorities of the National Security Division and I thank the FBI agents, DOJ prosecutors, and international partners who have put years of effort into this investigation."

"The complaint charges members of this North Korean-based conspiracy with being responsible for cyberattacks that caused unprecedented economic damage and disruption to businesses in the United States and around the globe," said First Assistant United States Attorney Tracy Wilkison. "The scope of this scheme was exposed through the diligent efforts of FBI agents and federal prosecutors who were able to unmask these sophisticated crimes through sophisticated means. They traced the attacks back to the source and mapped their commonalities, including similarities among the various programs used to infect networks across the globe. These charges send a message that we will track down malicious actors no matter how or where they hide. We will continue to pursue justice for those responsible for the huge monetary losses and attempting to compromise the national security of the United States."

"We will not allow North Korea to undermine global cybersecurity to advance its interests and generate illicit revenues in violation of our sanctions," said Treasury Secretary Steven Mnuchin. "The United States is committed to holding the regime accountable for its cyber-attacks and other crimes and destabilizing activities."

Park is charged with one count of conspiracy to commit computer fraud and abuse, which carries a maximum sentence of five years in prison, and one count of conspiracy to commit wire fraud, which carries a maximum sentence of 20 years in prison.

About the Defendant Park and Chosun Expo Joint Venture

According to the allegations contained in the criminal complaint, which was filed on June 8, 2018 in Los Angeles federal court, and posted today: Park Jin Hyok, was a computer programmer who worked for over a decade for Chosun Expo Joint Venture (a/k/a Korea Expo Joint Venture or "KEJV"). Chosun Expo Joint Venture had offices in China and the DPRK, and is affiliated with Lab 110, a component of DPRK military intelligence. In addition to the programming done by Park and his group for paying clients around the world, the Conspiracy also engaged in malicious cyber activities. Security researchers that have independently investigated these activities referred to this hacking team as the "Lazarus Group." The Conspiracy's methods included spear-phishing campaigns, destructive malware attacks, exfiltration of data, theft of funds from bank accounts, ransomware extortion, and propagating "worm" viruses to create botnets.

The Conspiracy's Cyber Attacks, Heists, and Intrusions

The complaint describes a broad array of the Conspiracy's alleged malicious cyber activities, both successful and unsuccessful, and in the United States and abroad, with a particular focus on four specific examples.

Targeting the Entertainment Industry

In November 2014, the conspirators launched a destructive attack on Sony Pictures Entertainment (SPE) in retaliation for the movie "The Interview," a farcical comedy that depicted the assassination of the DPRK's leader. The conspirators gained access to SPE's network by sending malware to SPE employees, and then stole confidential data, threatened SPE executives and employees, and damaged thousands of computers. Around the same time, the group sent spear-phishing messages to other victims in the entertainment industry, including a

movie theater chain and a U.K. company that was producing a fictional series involving a British nuclear scientist taken prisoner in DPRK.

Targeting Financial Services

In February 2016, the Conspiracy stole $81 million from Bangladesh Bank. As part of the cyber-heist, the Conspiracy accessed the bank's computer terminals that interfaced with the Society for Worldwide Interbank Financial Telecommunication (SWIFT) communication system after compromising the bank's computer network with spear-phishing emails, then sent fraudulently authenticated SWIFT messages directing the Federal Reserve Bank of NY to transfer funds from Bangladesh to accounts in other Asian countries. The Conspiracy attempted to and did gain access to several other banks in various countries from 2015 through 2018 using similar methods and "watering hole attacks," attempting the theft of at least $1 billion through such operations.

Targeting of U.S. Defense Contractors

In 2016 and 2017, the Conspiracy targeted a number of U.S. defense contractors, including Lockheed Martin, with spear-phishing emails. These malicious emails used some of the same aliases and accounts seen in the SPE attack, at times accessed from North Korean IP addresses, and contained malware with the same distinct data table found in the malware used against SPE and certain banks, the complaint alleges. The spear-phishing emails sent to the defense contractors were often sent from email accounts that purported to be from recruiters at competing defense contractors, and some of the malicious messages made reference to the Terminal High Altitude Area Defense (THAAD) missile defense system deployed in South Korea. The attempts to infiltrate the computer systems of Lockheed Martin, the prime contractor for the THAAD missile system, were not successful.

Creation of Wannacry 2.0

In May 2017, a ransomware attack known as WannaCry 2.0 infected hundreds of thousands of computers around the world, causing extensive damage, including significantly impacting the United Kingdom's National Health Service. The Conspiracy is connected to the development of WannaCry 2.0, as well as two prior versions of the ransomware, through similarities in form and function to other malware developed by the hackers, and by spreading versions of the ransomware through the same infrastructure used in other cyber-attacks.

Park and his co-conspirators were linked to these attacks, intrusions, and other malicious cyber-enabled activities through a thorough investigation that identified and traced: email and social media accounts that connect to each other and were used to send spear-phishing messages; aliases, malware "collector accounts" used to store stolen credentials; common malware code libraries; proxy services used to mask locations; and North Korean, Chinese, and other IP addresses. Some of this malicious infrastructure was used across multiple instances of the malicious activities described herein. Taken together, these connections and signatures—revealed in charts attached to the criminal complaint—show that the attacks and intrusions were perpetrated by the same actors.

Accompanying Mitigation Efforts

Throughout the course of the investigation, the FBI and the Department provided specific information to victims about how they had been targeted or compromised, as well as information about the tactics and techniques used by the conspiracy with the goals of remediating any intrusion and preventing future intrusions. That direct sharing of information took place in the United States and in foreign countries, often with the assistance of foreign law

enforcement partners. The FBI also has collaborated with certain private cybersecurity companies by sharing and analyzing information about the intrusion patterns used by the members of the conspiracy.

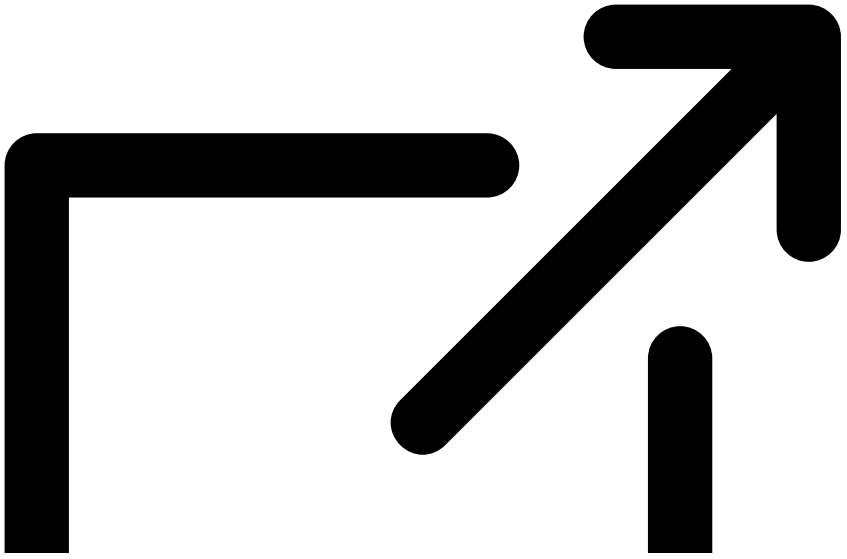
In connection with the unsealing of the criminal complaint, the FBI and prosecutors provided cybersecurity providers and other private sector partners detailed information on accounts used by the Conspiracy in order to assist these partners in their own independent investigative activities and disruption efforts.

The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only, as any sentencings of the defendant will be determined by the assigned judge.

This case is being prosecuted by Assistant United States Attorneys Stephanie S. Christensen, Anthony J. Lewis, and Anil J. Antony of the United States Attorney's Office for the Central District of California, and DOJ Trial Attorneys David Aaron and Scott Claffee of the National Security Division's Counterintelligence and Export Control Section. The Criminal Division's Office of International Affairs provided assistance throughout this investigation, as did many of the FBI's Legal Attachés, and foreign authorities around the world.

The charges contained in the criminal complaint are merely accusations and the defendant is presumed innocent unless and until proven guilty.

For the U.S. Department of Treasury's press release announcing corresponding sanctions please visit www.treasury.gov



.